


NETWORK ACCESS CONTROLLER AND ITS METHOD

Patent number: JP2002152279
Publication date: 2002-05-24
Inventor: SHITAMA KAZUHIRO
Applicant: SONY CORP
Classification:
 - international: H04L12/66; G06F13/00; H04L12/46; H04L12/28
 - european: H04L29/06C6A; H04L29/06C6C2
Application number: JP20000343429 20001110
Priority number(s): JP20000343429 20001110

Also published as:

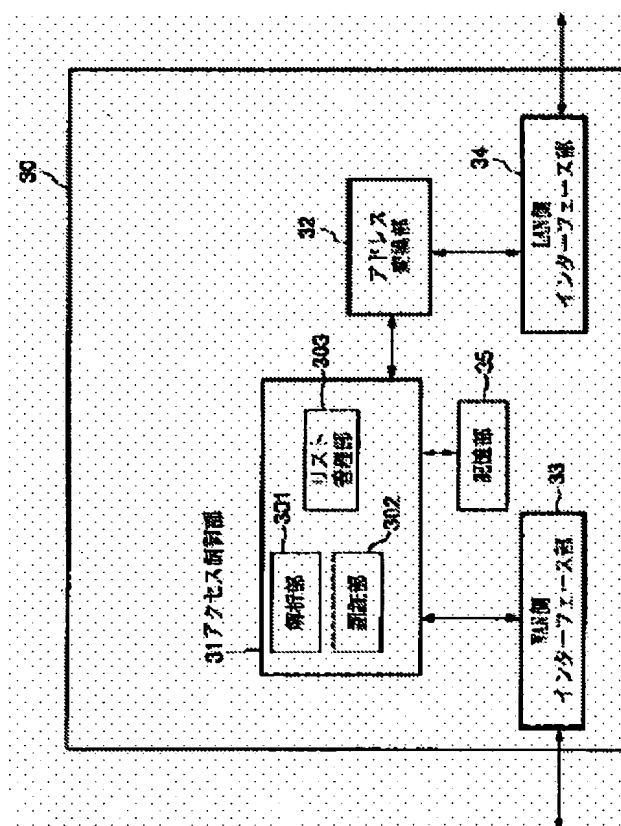
 US2002110123 (A)

Report a data error he

Abstract of JP2002152279

PROBLEM TO BE SOLVED: To provide a network access controller, that permits an access of an authenticated device on a global network to a device on a local network and can automatically control the permission setting of the access, and to provide its control method.

SOLUTION: An access control section 31 authenticates a device on the side of a global network transmitting an access request, generates an access permission entry to the authenticated device and adds the entry to an access permission list. Upon the receipt of a data packet from the device on the global network, the access control section 31 decides whether the data packet is to be transferred to the local network, on the basis of access information extracted from the data packet and access permission entry information included in the access permission list.



Data supplied from the esp@cenet database - Worldwide

(19) 日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-152279

(P2002-152279A)

(43) 公開日 平成14年5月24日 (2002.5.24)

(51) Int.Cl. ⁷	識別記号	FI	テマコード (参考)
H04L 12/66		G06F 13/00	351Z 5B089
G06F 13/00	351	H04L 11/20	B 5K030
H04L 12/46		11/00	310C 5K033
12/28			

審査請求 未請求 請求項の数9 OL (全10頁)

(21) 出願番号 特願2000-343429(P2000-343429)

(22) 出願日 平成12年11月10日 (2000.11.10)

(71) 出願人 000002185

ソニー株式会社

東京都品川区北品川6丁目7番35号

(72) 発明者 舌間 一宏

東京都品川区北品川6丁目7番35号 ソニー株式会社内

(74) 代理人 100094053

弁理士 佐藤 隆久

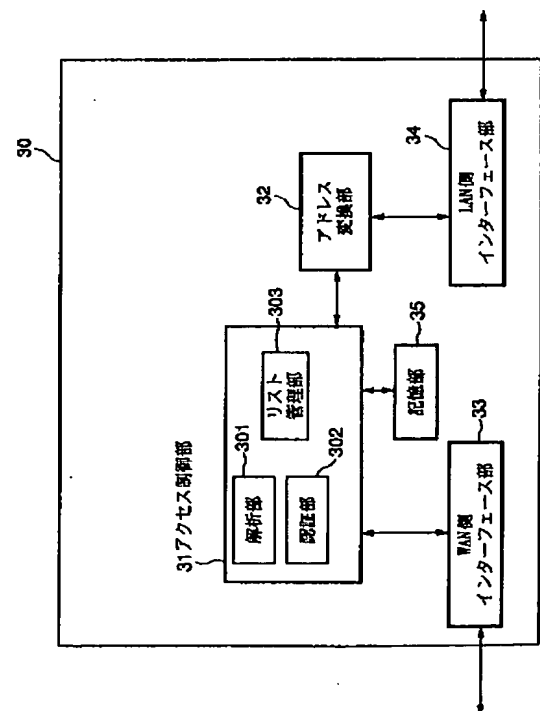
Fターム (参考) 5B089 GA21 GA31 HA06 KB03 KB06
 KB13 KC27 KG03
 5K030 GA15 HA08 HC14 HD03 HD06
 KA07 LC15 LC18 LD18 LD20
 5K033 AA08 CB06 CB08 DA05 DB12
 DB16 DB19 EC04

(54) 【発明の名称】 ネットワーク接続制御装置及びその方法

(57) 【要約】

【課題】 グローバルネットワークからローカルネットワーク上の機器へのアクセスを認証された機器に対して許可し、アクセスの許可設定を自動的に制御できるネットワーク接続制御装置及びその制御方法を実現する。

【解決手段】 アクセス制御部31によって、アクセス要求を送信したグローバルネットワーク側の機器に対して認証を行い、認証された機器に対しアクセス許可エントリを生成し、アクセス許可リストに追加する。アクセス制御部31はグローバルネットワーク側の機器からデータパケットを受信したとき、当該データパケットから抽出したアクセス情報と上記アクセス許可リストに含まれているアクセス許可エントリの情報とに基づき、当該データパケットをローカルネットワーク側に転送するかどうかを判断する。



(2)

1

【特許請求の範囲】

【請求項1】グローバルネットワーク側の機器からローカルネットワーク側が提供されているサービスにアクセスするとき、当該アクセスを許可または拒否する制御を行うネットワーク接続制御装置であって、上記グローバルネットワーク側の機器に対して認証を行う認証手段と、

上記認証手段によって認証された機器のアクセス要求に対して、アクセス許可エントリを生成し、当該アクセス許可エントリをアクセス許可リストに追加するアクセス許可エントリ作成手段と、

上記グローバルネットワーク側の機器からデータパケットを受信したとき、当該データパケットのヘッダから抽出した情報と上記アクセス許可リストに含まれているアクセス許可エントリとに基づき、当該データパケットをローカルネットワーク側に転送するか否かを判断する制御手段とを有するネットワーク接続制御装置。

【請求項2】上記エントリ作成手段は、上記認証された機器から送信されてきたアクセス要求パケットからアクセス情報を抽出し、送信元IPアドレス、宛先IPアドレス、送信元ポート番号、宛先ポート番号及び最終アクセス許可時刻を含むアクセス許可エントリを生成する請求項1記載のネットワーク接続制御装置。

【請求項3】上記制御手段は、上記グローバルネットワーク側の機器から送信されたデータパケットのヘッダから送信元IPアドレス、ポート番号及び宛先IPアドレス、ポート番号を抽出し、当該抽出した情報とアクセス許可リストに含まれているアクセス許可エントリの情報とを比較し、送信元IPアドレス、宛先IPアドレス、送信元ポート番号、宛先ポート番号がすべて一致した場合、当該データパケットをローカルネットワーク側に転送する請求項1記載のネットワーク接続制御装置。

【請求項4】上記制御手段は、上記グローバルネットワーク側の機器からのアクセス終了指示に従って、当該アクセスに対応するアクセス許可エントリを上記アクセス許可リストから削除する請求項1記載のネットワーク接続制御装置。

【請求項5】上記制御手段は、上記グローバルネットワーク側の機器から送信されてきたデータパケットの受信時刻に対応する、アクセス許可エントリに記憶されている最終アクセス許可時刻に基づき、最後のアクセスからの経過時間を算出し、当該経過時間が予め設定された基準時間を越えたとき、当該アクセス許可エントリを上記アクセス許可リストから削除する請求項1記載のネットワーク接続制御装置。

【請求項6】上記アクセス許可リストを記憶する記憶手段をさらに有する請求項1記載のネットワーク接続制御装置。

【請求項7】グローバルネットワーク側の機器からローカルネットワーク側が提供されているサービスにアクセ

2

スするとき、当該アクセスを許可または拒否する制御を行うネットワーク接続制御方法であって、

上記グローバルネットワーク側の機器に対して認証を行うステップと、

上記認証された機器のアクセス要求に対して、アクセス許可エントリを生成し、当該アクセス許可エントリをアクセス許可リストに追加するステップと、

上記グローバルネットワーク側の機器からデータパケットを受信したとき、当該データパケットのヘッダから抽出した情報と上記アクセス許可リストに含まれているアクセス許可エントリとに基づき、当該データパケットをローカルネットワーク側に転送するか否かを判断するステップとを有するネットワーク接続制御方法。

【請求項8】上記アクセス許可エントリを生成するとき、上記認証された機器から送信されてきたアクセス要求パケットからアクセス情報を抽出し、送信元IPアドレス、宛先IPアドレス、送信元ポート番号、宛先ポート番号及び最終アクセス許可時刻を含むアクセス許可エントリを生成する請求項7記載のネットワーク接続制御方法。

【請求項9】上記グローバルネットワーク側の機器から送信されたデータパケットのヘッダから送信元IPアドレス、送信元ポート番号、宛先IPアドレス、宛先ポート番号を抽出し、当該抽出した情報とアクセス許可リストに含まれているアクセス許可エントリの情報とを比較し、送信元IPアドレス、宛先のIPアドレス、送信先ポート番号、宛先ポート番号がすべて一致した場合、当該データパケットをローカルネットワーク側に転送する請求項7記載のネットワーク接続制御方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、グローバルネットワーク側の機器からローカルネットワーク側によって提供されているサービスにアクセスする場合においてそのアクセス許可を制御する制御装置及びその制御方法に関するものである。

【0002】

【従来の技術】ネットワークの普及に伴ってネットワークの利用者が急増し、また、ネットワーク上で様々な情報データを提供するサービス機関が増えつつある。ネットワークを用いて必要な情報を簡単に入手できる利便性が増える一方、不正なアクセスによる被害がネットワークの管理者にとって大きな問題となっている。WAN

(Wide Area Network) と呼ばれるグローバルネットワーク、例えば、インターネットなどからLAN (Local Area Network) と呼ばれるローカルネットワークへのアクセスを許可または不許可するなどの制御を行うファイアウォール機能を備えたゲートウェイはローカルネットワークに接続されているサーバ、端末機器のセキュリティを確保するには有効な手段である。

(3)

3

【0003】通常、ローカルネットワークからある特定のグローバルネットワーク上に設けられているネットワーク機器、例えば、ある特定の情報を提供するサーバへアクセスする場合、グローバルネットワークとローカルネットワークとの間に接続されているゲートウェイを介して行う。当該ゲートウェイには、グローバルネットワークに用いられるグローバルアドレスとローカルネットワークに用いられるローカルアドレスがそれぞれ割り当てられるほか、グローバルネットワークとローカルネットワークに接続されている端末機器との間にデータ通信を行うための通信ポートが付与されている。

【0004】インターネットなどのグローバルネットワーク側からの不正のアクセスを防止するために、ゲートウェイに設けられているファイアウォールは、インターネット側からのそれぞれのアクセスを許可または禁止する制御をシステム上の設定に従って、個別に行われている。この設定によって、デフォルト状態では特別に許可されていたアクセス先以外、すべてのアクセスが禁止される。これによって、ローカルネットワーク上の各サーバなどの端末機器にあるリソースを外部からの不正なアクセスによって破壊されたり、秘密事項の漏洩などを防止することができる。

【0005】しかし、このような措置を取られたことによって、正当なアクセスも拒否されるので、快適なインターネットサービスを一般のユーザに自由に提供できなくなり、サービスの利便性が損なわれる結果になりかねない。

【0006】ローカルネットワークのセキュリティ性を保ちつつ、外部からのアクセスを簡単に判別し、不正なアクセスを禁止し、正当なアクセスを許可するファイアウォールの改良技術が提案された。例えば、特許文献である公開特許公報「特開平11-338799」には、このような改良技術を開示している。この文献によって開示された技術によれば、グローバルネットワーク側の機器が、ファイアウォールが設けられている機器、例えば、所定の情報サービスを提供するサーバ（以下、これをローカルサーバと称する）にアクセスする場合に、まず、そのローカルネットワークのゲートウェイから、そのローカルサーバにアクセスするための移動コードをダウンロードする。そして、ダウンロードした移動コードを自分の機器で実行することで生成された中継エージェントを経由して、ローカルサーバに対してアクセスを行う。

【0007】この方法を採用することによって、従来のファイアウォールと同等のセキュリティレベルを維持しながら、グローバルネットワークからローカルサーバへのアクセスの利便性を向上させることが可能である。

【0008】

【発明が解決しようとする課題】ところで、上述した技術を用いる場合、ローカルサーバにアクセスする際に、

4

移動コードを事前にダウンロードする必要があり、また、この移動コードを実行して中継エージェントを生成するために、移動コードを実行する環境を予め用意しておかなければならないという不利益がある。

【0009】本発明は、かかる事情に鑑みてなされたものであり、その目的は、グローバルネットワークからローカルネットワーク上の機器へのアクセスを認証された機器に対して許可し、アクセスの許可設定を自動的に制御できるネットワーク接続制御装置及びその制御方法を提供することにある。

【0010】

【課題を解決するための手段】上記目的を達成するため、本発明のネットワーク接続制御装置は、グローバルネットワーク側の機器からローカルネットワーク側が提供されているサービスにアクセスするとき、当該アクセスを許可または拒否する制御を行うネットワーク接続制御装置であって、上記グローバルネットワーク側の機器に対して認証を行う認証手段と、上記認証手段によって認証された機器のアクセス要求に対して、アクセス許可エントリを生成し、当該アクセス許可エントリをアクセス許可リストに追加するアクセス許可エントリ作成手段と、上記グローバルネットワーク側の機器からデータパケットを受信したとき、当該データパケットのヘッダから抽出した情報と上記アクセス許可リストに含まれているアクセス許可エントリとに基づき、当該データパケットをローカルネットワーク側に転送するか否かを判断する制御手段とを有する。

【0011】また、本発明では、好適には、上記エントリ作成手段は、上記認証された機器から送信されてきたアクセス要求パケットからアクセス情報を抽出し、送信元IPアドレス、宛先IPアドレス、送信元ポート番号、宛先ポート番号及び最終アクセス許可時刻を含むアクセス許可エントリを生成する。

【0012】また、本発明では、好適には、上記制御手段は、上記グローバルネットワーク側の機器から送信されたデータパケットのヘッダから送信元IPアドレス、ポート番号及び宛先IPアドレス、ポート番号を抽出し、当該抽出した情報とアクセス許可リストに含まれているアクセス許可エントリの情報とを比較し、送信元IPアドレス、宛先IPアドレス、送信元ポート番号、宛先ポート番号がすべて一致した場合、当該データパケットをローカルネットワーク側に転送する。

【0013】また、本発明では、好適には、上記制御手段は、上記グローバルネットワーク側の機器からのアクセス終了指示に従って、当該アクセスに対応するアクセス許可エントリを上記アクセス許可リストから削除する。

【0014】また、本発明では、好適には、上記制御手段は、上記グローバルネットワーク側の機器から送信されてきたデータパケットの受信時刻に対応する、アクセ

(4)

5

ス許可エントリに記憶されている最終アクセス許可時刻に基づき、最後のアクセスからの経過時間を算出し、当該経過時間が予め設定された基準時間を越えたとき、当該アクセス許可エントリを上記アクセス許可リストから削除する。

【0015】また、本発明のネットワーク接続制御方法は、グローバルネットワーク側の機器からローカルネットワーク側が提供されているサービスにアクセスするとき、当該アクセスを許可または拒否する制御を行うネットワーク接続制御方法であって、上記グローバルネットワーク側の機器に対して認証を行うステップと、上記認証された機器のアクセスに対して、アクセス許可エントリを生成し、当該アクセス許可エントリをアクセス許可リストに追加するステップと、上記グローバルネットワーク側の機器からデータパケットを受信したとき、当該データパケットのヘッダから抽出した情報と上記アクセス許可リストに含まれているアクセス許可エントリとに基づき、当該データパケットをローカルネットワーク側に転送するか否かを判断するステップとを有する。

【0016】また、本発明では、好適には、上記アクセス許可エントリを生成するとき、上記認証された機器から送信されてきたアクセス要求パケットからアクセス情報を抽出し、送信元IPアドレス、宛先IPアドレス、送信元ポート番号、宛先ポート番号及び最終アクセス許可時刻を含むアクセス許可エントリを生成する。

【0017】さらに、本発明では、好適には、上記グローバルネットワーク側の機器から送信されたデータパケットのヘッダから送信元IPアドレス、送信元ポート番号、宛先IPアドレス、宛先ポート番号を抽出し、当該抽出した情報とアクセス許可リストに含まれているアクセス許可エントリの情報とを比較し、送信元IPアドレス、宛先のIPアドレス、送信先ポート番号、宛先ポート番号がすべて一致した場合、当該データパケットをローカルネットワーク側に転送する。

【0018】

【発明の実施の形態】第1実施形態

図1は本発明に係るネットワーク接続制御装置を含むネットワークシステムの一例を示す構成図である。図示のように、このネットワークシステムは、グローバルネットワーク(WAN: Wide Area Network) 10、ローカルネットワーク(LAN: Local Area Network) 20、グローバルネットワーク10とローカルネットワークとの間に接続されているゲートウェイ30、グローバルネットワーク10に接続されている端末機器40、及びローカルネットワーク20に接続されている端末機器50によって構成されている。

【0019】ゲートウェイ30は、グローバルネットワーク10側の端末機器から、ローカルネットワーク20側で提供されているサービスへのアクセス要求を受けたとき、認証された端末機器のみに対して、そのアクセス

6

を許可するファイアウォール機能を有するいわゆるネットワーク接続制御装置である。なお、図1では、グローバルネットワーク10及びローカルネットワーク20に、それぞれ一つずつ端末機器が接続されているが、実際のネットワークシステムでは、通常グローバルネットワーク10及びローカルネットワーク20にはそれぞれ多数の端末機器が接続されている。

【0020】ゲートウェイ30には、ファイアウォールが設けられており、通常ではグローバルネットワーク10側の端末機器からローカルネットワーク20側の端末機器へのアクセスを許可しない。また、ローカルネットワーク20の内部では、各端末機器にそれぞれプライベートのIPアドレスが割り当てられており、ゲートウェイ30のグローバルネットワーク接続インターフェースには、グローバルなIPアドレスが少なくとも一つ割り当てられている。ローカルネットワーク20側の各端末機器は、IPマスカレード技術を用いてグローバルネットワーク側の提供するサービスにアクセスする。

【0021】本発明は、このように構成されているネットワークシステムにグローバルネットワーク10に接続されている端末機器のうち、認証された機器からのアクセス要求により、その機器のみ指定したローカルネットワーク20側のサービスへのアクセスを許可し、他のグローバルネットワーク側の機器からのアクセスを拒否する、即ちファイアウォール設定を動的に変更可能なネットワーク接続制御装置を提供する。

【0022】なお、以下の説明では、グローバルネットワーク10側の端末機器が希望するサービスをゲートウェイ30に通知する際のメッセージを便宜上“サービスアクセス要求メッセージ”という。また、ローカルネットワーク20側では、プライベートIPアドレスが用いられているため、ローカルネットワーク20側によって提供されているサービスをグローバルネットワーク側の機器から指定できるように、各サービスごとにゲートウェイ30にポート番号が割り当てられている。グローバルネットワーク10側の機器は、ゲートウェイ30におけるグローバルネットワーク側のインターフェースのグローバルIPアドレスとそのポート番号を指定することによって、希望するサービスにアクセスできる。

【0023】ここで、グローバルネットワーク側の機器がローカルネットワーク側のサービスを指定するためのIPアドレスとポート番号を便宜上それぞれ“サービスIPアドレス”と“サービスポート番号”と呼び、グローバルネットワーク側の機器がローカルネットワーク側の機器にアクセスするとき、これらのサービスIPアドレスとサービスポート番号とをサービスアクセス要求メッセージに組み込み、ゲートウェイ30に送信する。

【0024】図2は、ゲートウェイ30の構成を示すブロック図である。以下、図2を参照しつつ、ゲートウェイ30の各部分の構成及び機能について説明する。図示

(5)

7

のように、ゲートウェイ30は、アクセス制御部31、アドレス変換部32、グローバルネットワーク（WAN）側インターフェース部33、ローカルネットワーク（LAN）側インターフェース部34、及び記憶部35によって構成されている。さらに、アクセス部31は、解析部301、認証部302及びリスト管理部303によって構成されている。

【0025】アクセス制御部31は、グローバルネットワーク側から受信したサービスアクセス要求メッセージを解析し、機器の認証を行い、アクセス許可リストの管理を行う。また、その解析及び認証の結果に応じて、グローバルネットワーク側から受信したデータパケットのアクセスの許可または拒否を制御する。

【0026】以下、アクセス制御部31の各構成部分について説明する。解析部301は、WAN側インターフェース部33によって受信したデータパケットから必要な情報を抽出して解析を行う。例えば、グローバルネットワーク側の機器からローカルネットワーク側の機器に対して、サービスアクセス要求メッセージが送信されると、このメッセージがWAN側インターフェース部33によって受け取って、アクセス制御部31に渡される。アクセス制御部31において、解析部301によって、受信したサービスアクセス要求メッセージから、送信元IPアドレス、ポート番号及び宛先IPアドレス、ポート番号などの情報が抽出され、それに基づいてアクセス許可エントリが生成され、リスト管理部303に送られる。

【0027】また、解析部301は、WAN側インターフェース部33によって受信したデータパケットのヘッダから送信元及び宛先のIPアドレス、ポート番号などの情報を抽出し、当該抽出した情報とアクセス許可リストに含まれるアクセス許可エントリの情報に基づき、アクセスの許可または拒否を決定する。

【0028】認証部302は、グローバルネットワーク10側の機器からサービスアクセス要求メッセージを受けたとき、当該機器に対して予め設定された認証方法及び認証手順に従って認証を行う。そして、認証された機器に関する情報を解析部301に送信し、解析部301によってそのアクセスに対するアクセス許可エントリが作成される。

【0029】リスト管理部303は、解析部301によって作成されたアクセス許可エントリを受け取り、記憶部35に記憶されたアクセス許可リストに追加する。または、アクセス終了したとき、記憶部35に記憶されたアクセス許可リストからそのアクセスに対応するアクセス許可エントリを削除する。

【0030】アドレス変換部32は、ローカルネットワーク20側にプライベートIPアドレス（または、ローカルIPアドレスという）が使用されている場合のみに必要である。即ち、アドレス変換部32は、グローバル

8

ネットワーク10側で使用されているグローバルIPアドレスとローカルネットワーク20側で使用されているローカルIPアドレスとを変換する。

【0031】WAN側インターフェース33は、グローバルネットワーク10に対してパケットの送受信を行う。即ち、グローバルネットワーク10から送信されてきたパケットを受信して、アクセス制御部31に送り、また、アクセス制御部31によって生成されたパケットをグローバルネットワーク10に送信する。

10 【0032】LAN側インターフェース34は、ローカルネットワーク20に対してパケットの送受信を行う。即ち、ローカルネットワーク20から送信されてきたパケットを受信して、アドレス変換部32に送り、また、アドレス変換部32から送られてきたパケットをローカルネットワーク20に送信する。

【0033】記憶部35は、アクセス許可リストを記憶する。当該アクセス許可リストは、アクセス制御部31のリスト管理部によって管理される。解析部301によって生成されたアクセス許可エントリが当該アクセス許可リストに追加され、また、終了したアクセスのアクセス許可エントリが当該アクセス許可リストから削除される。

20 【0034】以下、本実施形態におけるゲートウェイ30のアクセス制御部31の動作について説明する。まず、グローバルネットワーク10側の機器から“サービスIPアドレス”と“サービスポート番号”が記載された“サービスアクセス要求メッセージ”をWAN側インターフェース部33から受信したときにアクセス制御部31の動作について説明する。

30 【0035】図3は“サービスアクセス要求メッセージ”を受信したときのアクセス制御部31の動作を示すフローチャートである。図3に示すように、まず、WAN側インターフェース部33から受信したサービスアクセス要求メッセージを受け取る（ステップS1）。そして、受信したサービスアクセス要求メッセージのIPヘッダに記載されている送信側の機器とインターフェースを示す始点IPアドレスと始点ポート番号を確認し、当該サービスアクセス要求メッセージを送信した機器について認証を行う（ステップS2）。なお、ここで、機器を認証する方法は、IPsec AHによる認証と、ケルベロスによる第3者認証などが考えられるが、本発明では、この送信側機器の認証は、既存の方法によって実現できるので、特に限定しない。

40 【0036】認証に失敗した場合は、その“サービスアクセス要求メッセージ”を廃棄して（ステップS3）、処理を終了する。逆に認証に成功した場合に、次に示す処理が行われる。

50 【0037】認証が成功した場合、その“サービスアクセス要求メッセージ”からIPヘッダの始点アドレス、IPヘッダ始点ポート番号、ペイロードに記載されてい

(6)

9

るサービスIPアドレス番号、及びペイロードに記載されているサービスポート番号の4つの情報がそれぞれ抽出される。

【0038】そして、上記抽出された4つの情報をそれぞれ許可始点IPアドレスフィールド(ASIP)、許可終点IPアドレスフィールド(ADIP)、許可始点ポート番号フィールド(ASPT)、及び許可終点ポート番号フィールド(ADPT)の4つの記憶領域(フィールド)にそれぞれ格納して、“アクセス許可エントリ”を作成する(ステップS4)。

【0039】アクセス許可エントリには、上述した4つのフィールド以外に、このエントリを用いてグローバルネットワーク10側から、ローカルネットワーク20側へパケットを最後に中継したときの時刻を格納する“最終アクセス許可時刻フィールド(LATM)”があり、新規作成のときは、そのアクセス許可エントリを作成した時刻が当該フィールドに格納されている。

【0040】そして、上述したように作成した“アクセス許可エントリ”を“アクセス許可リスト”に追加する(ステップS5)。

【0041】図4には、上述した処理によって生成されたアクセス許可エントリの一例を示している。図示のように、当該エントリにおいて、許可始点IPアドレスフィールド(ASIP)には、サービスアクセス要求メッセージを送信した機器のグローバルIPアドレス、例えば、131.113.82.1が格納され、許可終点IPアドレスフィールド(ADIP)には、サービスアクセス要求メッセージの宛先を示すアドレス、例えば、ゲートウェイ30のWAN側のインターフェース部33に割り当てられているグローバルIPアドレス、210.139.255.223が格納されている。また、許可始点ポート番号フィールド

(ASPT)には、サービスアクセス要求メッセージを送信した機器のポート番号、例えば、20010が格納され、さらに、許可終点ポート番号フィールド(ADPT)には、サービスアクセス要求メッセージの宛先を示すポート番号、ここで、例えば、5000が格納されている。また、最終アクセス許可時刻フィールド(LATM)には、エントリを作成した時刻である21:10:10が格納されている。

【0042】図4に示すアクセス許可エントリがアクセス許可リストに追加される。なお、当該アクセス許可リストは、アクセス制御部31によって管理されており、例えば、記憶部35に記憶されている。

【0043】次に、WAN側インターフェース部33によって、グローバルネットワーク10からデータパケットを受信したときアクセス制御部33の動作について、図5に示すフローチャートを参照しつつ説明する。

【0044】まず、WAN側インターフェース部33からデータパケットを受け取る(ステップS1)。受信したデータパケットから、IPヘッダの始点IPアドレ

10

ス(SIP)、IPヘッダの終点IPアドレス(DIP)、TCP/UDPヘッダの始点ポート番号(SPT)、及びTCP/UDPヘッダの終点ポート番号(DPT)を4つの情報をそれぞれ抽出する。

【0045】そして、記憶部35に保持されているアクセス許可リストを参照して、ASIPがSIPに等しく、ADIPがDIPに等しく、ASPTがSPTに等しく、さらにADPTがDPTに等しいアクセス許可エントリが存在するか否かについて確認する。当該確認の結果に従って、受信したデータパケットに対して通過の許可または拒否を決定する(ステップS2)。

【0046】上記の確認において、すべてのフィールドが一致しない場合、データパケットの通過が許可されず、このデータパケットが廃棄される(ステップS3)。

【0047】一方、上記の確認において、すべてのフィールドが一致するアクセス許可エントリが存在する場合、受信したデータパケットの通過が許可される。このとき、該当するアクセス許可エントリの最終アクセス許可時刻フィールド(LATM)には、現在の時刻が格納される(ステップS4)。なお、ここでいう現在の時刻は、例えば、ゲートウェイ30のOS(オペレーションシステム)によって管理され、通常システム時計と呼ばれる時間管理部によって示されている時間である。

【0048】最終アクセス許可時刻フィールドを更新したあと、受信したデータパケットがアドレス変換部32に転送される(ステップS5)。そして、アドレス変換部32において、データパケットのIPヘッダにあるグローバルIPアドレスがローカルネットワーク20の内部で使用されているローカルIPアドレスに変換され、LAN側インターフェース部34に転送される。具体的に、例えば、DIP及びDPTがそれぞれローカルネットワーク20側で実際にサービスを提供している機器のローカルIPアドレス及びポート番号に変換される。変換されたデータパケットがLAN側インターフェース部34によってローカルネットワーク20に送信され、実際にサービスを提供している機器に転送される。

【0049】上述した処理によって、グローバルネットワーク10側の機器からローカルネットワーク20によって提供されているサービスにアクセスしようとする場合、ゲートウェイ30によって受信したデータパケットのIPヘッダ及びTCP/UDPヘッダに含まれている始点と終点IPアドレス及び始点と終点ポート番号情報が抽出され、当該抽出された情報と記憶部35に記憶されているアクセス許可リストとの比較結果に基づき、アクセスを許可または拒否するかが決定される。当該アクセスが拒否された場合、データパケットが廃棄され、逆に当該アクセスが許可された場合、アドレス変換部32によって、データパケットの宛先がローカルネットワーク20で使用されているサービス提供する機器のローカ

(7)

11

ルIPアドレスに変換され、LAN側インターフェース部34を介してローカルネットワーク20側に転送される。

【0050】このため、グローバルネットワーク10側の機器からローカルネットワーク20側によって提供されているサービスにアクセスする場合、認証された機器からのアクセスのみが許可され、それ以外の機器からのアクセスが拒否されるので、ファイアウォールのセキュリティ性が向上し、不正がアクセスを拒否できるほか、認証された機器からのアクセスが許可され、正規のユーザに対して利便性の高いサービスを提供することができる。

【0051】上述した処理によって、記憶部35に許可されたアクセスのアクセス許可エントリによって形成されたアクセス許可リストが記憶される。ゲートウェイ30において、当該アクセス許可リストと受信されたデータパケットのIPヘッダ及びTCP/UDPヘッダ情報に基づき、受信されたデータパケットをローカルネットワーク20側に送信するか否かの判断が行われる。アクセスが確立するたびにそのアクセスに対して新しいアクセス許可エントリが作成され、アクセス許可リストに追加されるので、アクセス許可リストの容量が受けたアクセスの数に従って増えていく。さらに、アクセス許可エントリをそのままアクセス許可リストに残すと、一回認証を受けたアクセスに関するアクセス許可エントリが、たとえそのアクセスが終了した場合でも記憶部35のアクセス許可リストに永久に残ってしまうため、セキュリティ上問題がある。このため、終了したアクセスに対してそのアクセス許可エントリを随時削除する必要がある。

【0052】図6は最終アクセス許可時刻とスレッシュールド時間に基づきアクセス許可エントリを削除する処理を示すフローチャートである。以下、図6を参照し、アクセス許可エントリの削除処理について説明する。

【0053】この削除処理は、最終アクセス許可時刻から現在（判断時）の時刻までの経過時間 t_D と予め設定されたスレッシュールド時間 T_S とを比較し、比較の結果経過時間 t_D がスレッシュールド時間 T_S を越えたとき、そのアクセス許可エントリをアクセス許可リストから削除する。即ち、最後のアクセスから一定の時間を経過しても新たなアクセスがなかった場合、そのアクセスに対する許可が取り消される。なお、この削除処理は、ある一定時間ごとに、アクセス許可リスト中全エントリに対して実行される。

【0054】図6に示すように、まず、アクセス許可エントリから最終アクセス許可時刻フィールド(LATM)の値 t_f が読み出される(ステップSP1)。そして、現時刻 t と最終アクセス許可時刻フィールドから読み出した時刻 t_f との差、即ち、最終アクセス許可時刻から現在までの経過時間 t_D ($=t-t_f$)が計算され

12

る。当該経過時間 t_D とスレッシュールド時間 T_S とが比較される(ステップSP2)。

【0055】経過時間 t_D がスレッシュールド時間 T_S より小さい場合、そのアクセス許可エントリに対して何にも処理しない(ステップSP3)。経過時間 t_D がスレッシュールド時間 T_S と等しく、またはより大きい場合、そのアクセス許可エントリがアクセス許可リストから削除される(ステップSP4)。

【0056】上述した処理によって最終アクセス時間からの経過時間 t_D が所定のスレッシュールド時間 T_S を越えたとき、そのアクセス許可エントリはアクセス許可リストから削除される。即ち、最終アクセスから一定の時間を経過してアクセスがなかった場合、そのアクセスを終了したものと見なして、アクセス許可エントリが削除される。なお、スレッシュールド時間 T_S をアクセス許可エントリごとに異なる値に設定することができる。例えば、WWWサーバへのアクセスに関して、アクセス許可エントリのスレッシュールド時間 T_S を短く設定し、TelnetやFTPに関するアクセス許可エントリのスレッシュールド時間 T_S を長く設定することができる。

【0057】図7は、アクセスする側からアクセス終了の通知を受けた場合、そのアクセスに対して形成されたアクセス許可エントリをアクセス許可リストから削除する処理を示すフローチャートである。以下、図7を参照しつつ、この削除処理について説明する。

【0058】図示のように、まず、WAN側インターフェース部33からデータパケットが受け取られる(ステップSQ1)。次に、受け取ったデータパケットに終了を示す情報(以下、便宜上アクセス終了情報という)が含まれているか否かについて判断が行われる(ステップSQ2)。

【0059】当該判断の結果、アクセス終了情報が含まれていない場合、データパケットに対して通常の処理が行われる(ステップSQ3)。一方、当該判断の結果、データパケットにアクセス終了情報が含まれている場合、当該アクセスに応じたアクセス許可エントリがアクセス許可リストから削除される(ステップSQ4)。

【0060】上述した処理によって、受信したデータパケットにアクセス終了情報が含まれている場合、そのアクセスが確立したときに形成されたアクセス許可エントリがアクセス許可リストから削除される。このため、グローバルネットワーク10側の機器からアクセスの終了が指示された場合、これに従ってアクセスが終了した時点でそのアクセスが確立した時点で形成されていたアクセス許可エントリがすぐアクセス許可リストから削除されるので、アクセス終了後、そのエントリが悪用されることが防止でき、セキュリティ上好ましい。

【0061】また、アクセス許可リスト中のアクセス許可エントリ数は、ゲートウェイ30のリソースが有限であるため、ある一定値を越えると格納できなくなる。

(8)

13

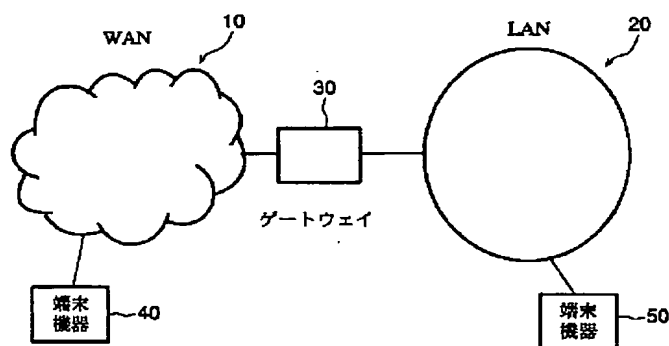
このため、アクセス許可エントリの数が最大の状況で新規のアクセス許可エントリが追加されたとき、保持しているアクセス許可リストの中から、アクセス許可エントリの最終アクセス許可時刻の値がもっとも古いアクセス許可エントリを削除し、新規のアクセス許可エントリを追加することができる。

【0062】以上、本実施形態のネットワーク接続制御装置、即ちゲートウェイ30における2種類のエントリ削除処理について説明したが、ゲートウェイ30のエントリ削除処理は、これに限られることなく、他の処理によって行われることもできる。例えば、ゲートウェイ30の判断に基づきアクセスを強制的に終了させる処理、あるいはローカルネットワーク側に実際にサービスを提供している機器の判断に基づき、アクセスを終了させることも考えられる。

【0063】

【発明の効果】以上説明したように、本発明のネットワーク接続制御装置及びその制御方法によれば、ファイアウォール機能を備えたゲートウェイにおいて、許可されたグローバルネットワーク側の機器のみがローカルネットワーク側のサービスにアクセスすることが許可され、ネットワーク利用者は必要に応じて移動先のネットワークからあるローカルネットワークによって提供されているサービスを容易に利用できる。一方、他の利用者の機器からのアクセスを、ゲートウェイのファイアウォールの設定によって拒否することができ、ローカルネットワ

【図1】



14

ーク側のセキュリティレベルを維持できる利点がある。

【図面の簡単な説明】

【図1】本発明に係るネットワーク接続制御装置（ゲートウェイ）を用いたネットワークシステムの一構成例を示す図である。

【図2】ゲートウェイの構成を示すブロック図である。

【図3】グローバルネットワーク側の機器からアクセス要求を受信したとき、アクセス制御部の動作を示すフローチャートである。

10 【図4】アクセス許可エントリの一例を示す図である。

【図5】グローバルネットワークからデータパケットを受信したときのアクセス制御部の動作を示すフローチャートである。

【図6】最終許可時刻とスレッシュホールド時間に基づきアクセス許可エントリを削除する処理を示すフローチャートである。

【図7】アクセスする側からのアクセス終了通知に応じてアクセス許可エントリを削除する処理を示すフローチャートである。

20 【符号の説明】

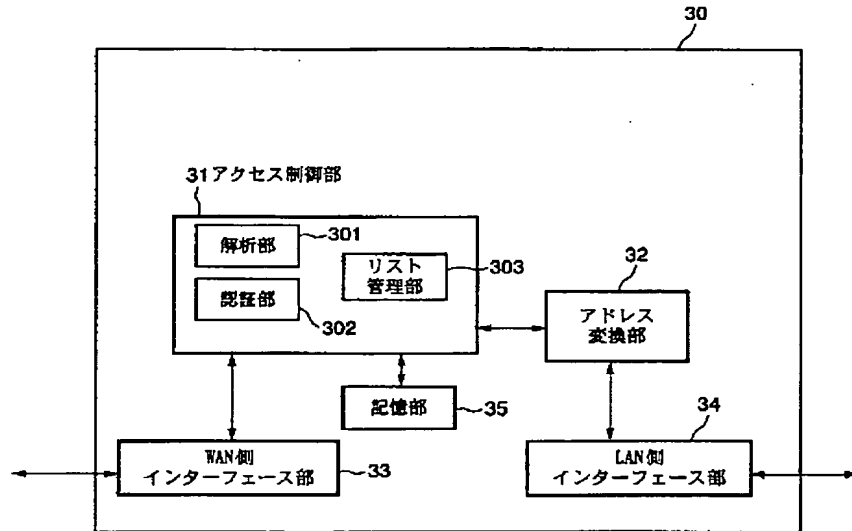
10…グローバルネットワーク、20…ローカルネットワーク、30…ゲートウェイ、31…アクセス制御部、301…解析部、302…認証部、303…リスト管理部、32…アドレス変換部、33…WAN側インターフェース部、34…LAN側インターフェース部、35…記憶部、40、50…端末機器。

【図4】

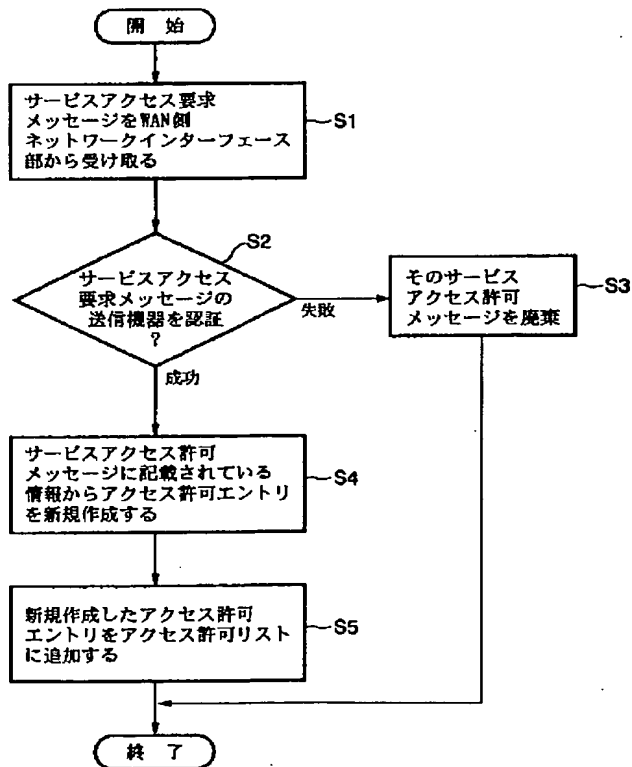
ASIP	131.113.82.1
ADIP	210.139.255.223
ASPT	20010
ADPT	5000
LATM	21:10:10

(9)

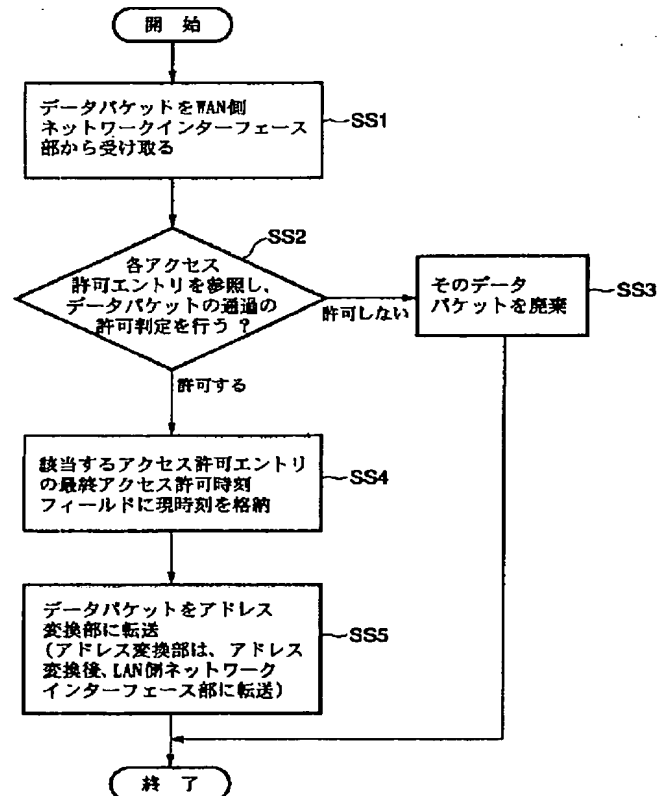
【図2】



【図3】

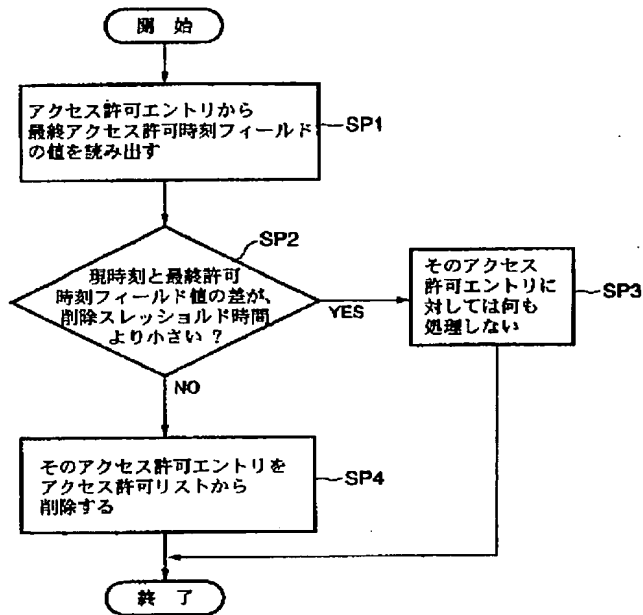


【図5】

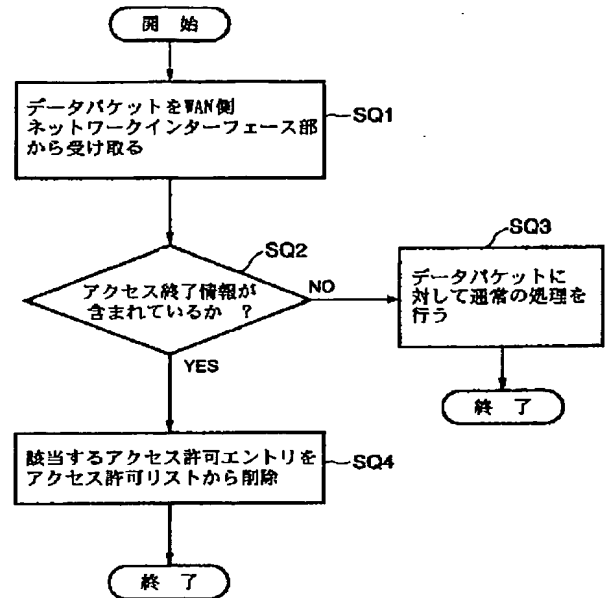


(10)

【図6】



【図7】



* NOTICES *

JPO and NCIPi are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] When accessing the service currently provided with the local network side from the device by the side of global network, The authentication means which is the network connection control device which performs control which permits or refuses the access concerned, and attests to the device by the side of the above-mentioned global network, An access-permission entry creation means to generate an access-permission entry and to add the access-permission entry concerned to an access permit list to the access request of the device attested by the above-mentioned authentication means, When a data packet is received from the device by the side of the above-mentioned global network, The network connection control unit which has the control means which judges whether the data packet concerned is transmitted to a local network side based on the information extracted from the header of the data packet concerned, and the access-permission entry contained in the above-mentioned access permit list.

[Claim 2] The above-mentioned entry creation means is a network connection control unit according to claim 1 which generates the access-permission entry which extracts access information from the access request packet transmitted from the device by which authentication was carried out [above-mentioned], and contains a transmitting agency IP address, a destination IP address, a transmitting agency port number, a destination port number, and the last access-permission time of day.

[Claim 3] The above-mentioned control means is a network connection control unit according to claim 1 which transmits the data packet concerned to a local network side when a transmitting agency IP address, a port number and a destination IP address, and a port number are extracted from the header of the data packet transmitted from the device by the side of the above-mentioned global network, the extracted information concerned is compared with the information on the access-permission entry contained in the access permit list and all of a transmitting agency IP address, a destination IP address, a transmitting agency port number, and a destination port number are in agreement.

[Claim 4] The above-mentioned control means is a network connection control unit according to claim 1 which deletes the access-permission entry corresponding to the access concerned from the above-mentioned access permit list according to the access termination directions from the device by the side of the above-mentioned global network.

[Claim 5] The above-mentioned control means is a network connection control unit according to claim 1 which deletes the access-permission entry concerned from the above-mentioned access permit list when the elapsed time from the last access is computed and the elapsed time concerned exceeds the conventional time set up beforehand based on the last access-permission time of day corresponding to the receipt time of the data packet transmitted from the device by the side of the above-mentioned global network memorized by the access-permission entry.

[Claim 6] The network connection control unit according to claim 1 which has further a storage means to memorize the above-mentioned access permit list.

[Claim 7] When accessing the service currently provided with the local network side from the device by the side of global network, The step which is the network connection control approach of performing control which permits or refuses the access concerned, and attests to the device by the side of the above-

mentioned global network, The step which generates an access-permission entry and adds the access-permission entry concerned to an access permit list to the access request of the device by which authentication was carried out [above-mentioned], When a data packet is received from the device by the side of the above-mentioned global network, The network connection control approach of having the step which judges whether the data packet concerned being transmitted to a local network side based on the information extracted from the header of the data packet concerned, and the access-permission entry contained in the above-mentioned access permit list.

[Claim 8] The network connection control approach according to claim 7 which generates the access-permission entry which extracts access information from the access request packet transmitted from the device by which authentication was carried out [above-mentioned] when generating the above-mentioned access-permission entry, and contains a transmitting agency IP address, a destination IP address, a transmitting agency port number, a destination port number, and the last access-permission time of day.

[Claim 9] The network connection control approach according to claim 7 of transmitting the data packet concerned to a local network side when a transmitting agency IP address, a transmitting agency port number, a destination IP address, and a destination port number are extracted from the header of the data packet transmitted from the device by the side of the above-mentioned global network, the extracted information concerned is compared with the information on the access-permission entry contained in the access permit list and all of a transmitting agency IP address, the IP address of the destination, a transmission place port number, and a destination port number are in agreement.

[Translation done.]

* NOTICES *

JPO and NCIPI are not responsible for any damages caused by the use of this translation.

- 1.This document has been translated by computer. So the translation may not reflect the original precisely.
- 2.**** shows the word which can not be translated.
- 3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the control unit which controls the access permission, and its control approach, when accessing the service currently offered by the local network side from the device by the side of global network.

[0002]

[Description of the Prior Art] The service establishments which a network user increases rapidly with the spread of network, and offer various information data on a network are increasing in number. While the convenience which can obtain required information easily using a network increases, it has been the problem for a network manager that the damage by unjust access is big. They are the server by which the gateway equipped with authorization or the fire wall function which controls carrying out disapproval etc. is connected to the local network in access to the local network called LAN (Local Area Network) from the global network called WAN (Wide Area Network), for example, the Internet etc., and a means effective in securing the security of a terminal equipment.

[0003] Usually, when accessing to the network device prepared on a certain specific global network from the local network, for example, the server which offers a certain specific information, it carries out through the gateway connected between global network and a local network. In the gateway concerned, the global address used for global network and the local address used for a local network are assigned, respectively, and also the communication link port for performing data communication is given between the terminal equipments connected to global network and a local network.

[0004] In order to prevent unjust access from a global-network side, such as the Internet, the fire wall prepared in the gateway is performed according to the individual according to the setup on a system in the control which permits or forbids each access from the Internet side. By this setup, all accesses are forbidden by the default except the access place permitted specially. By this, unjust access from the outside can destroy the resource in terminal equipments, such as each server on a local network, or leakage of a secret matter etc. can be prevented.

[0005] However, since just access is also refused by having taken such a measure, a result it becomes impossible to provide a general user with the comfortable Internet service freely and by which the convenience of service is spoiled may be brought.

[0006] Maintaining the security nature of a local network, access from the outside was distinguished simply, unjust access was forbidden, and the amelioration technique of the fire wall which permits just access was proposed. For example, such an amelioration technique is indicated in the open patent official report "JP,11-338799,A" which is patent reference. When the device by the side of global network accesses the device by which the fire wall is prepared, for example, the server which offers predetermined data utility, (this is hereafter called a local server) according to the technique indicated with this reference, the migration code for accessing that local server is first downloaded from the gateway of that local network. And the downloaded migration code is accessed to a local server via the junction agent generated by performing by its own device.

[0007] It is possible to raise the convenience of access to a local server from global network, maintaining security level equivalent to the conventional fire wall by adopting this approach.

[0008]

[Problem(s) to be Solved by the Invention] By the way, in order to download a migration code in advance, and to perform this migration code and to generate a junction agent in case a local server is accessed when using the technique mentioned above, there is disadvantageous profit that the environment where a migration code is performed must be prepared beforehand.

[0009] This invention is made in view of this situation, the purpose is permitted to the device which had access to the device on a local network from global network attested, and it is in offering the network connection control unit which can control an authorization setup of access automatically, and its control approach.

[0010]

[Means for Solving the Problem] In order to attain the above-mentioned purpose, the network connection control unit of this invention When accessing the service currently provided with the local network side from the device by the side of global network, The authentication means which is the network connection control device which performs control which permits or refuses the access concerned, and attests to the device by the side of the above-mentioned global network, An access-permission entry creation means to generate an access-permission entry and to add the access-permission entry concerned to an access permit list to the access request of the device attested by the above-mentioned authentication means, When a data packet is received from the device by the side of the above-mentioned global network, Based on the information extracted from the header of the data packet concerned, and the access-permission entry contained in the above-mentioned access permit list, it has the control means which judges whether the data packet concerned is transmitted to a local network side.

[0011] Moreover, in this invention, suitably, the above-mentioned entry creation means extracts access information from the access request packet transmitted from the device by which authentication was carried out [above-mentioned], and generates the access-permission entry containing a transmitting agency IP address, a destination IP address, a transmitting agency port number, a destination port number, and the last access-permission time of day.

[0012] Moreover, in this invention, suitably, the above-mentioned control means transmits the data packet concerned to a local network side, when a transmitting agency IP address, a port number and a destination IP address, and a port number are extracted from the header of the data packet transmitted from the device by the side of the above-mentioned global network, the extracted information concerned is compared with the information on the access-permission entry contained in the access permit list and all of a transmitting agency IP address, a destination IP address, a transmitting agency port number, and a destination port number are in agreement.

[0013] Moreover, in this invention, the above-mentioned control means deletes the access-permission entry corresponding to the access concerned from the above-mentioned access permit list suitably according to the access termination directions from the device by the side of the above-mentioned global network.

[0014] Moreover, in this invention, suitably, the above-mentioned control means computes the elapsed time from the last access based on the last access-permission time of day corresponding to the receipt time of the data packet transmitted from the device by the side of the above-mentioned global network memorized by the access-permission entry, and when the elapsed time concerned exceeds the conventional time set up beforehand, it deletes the access-permission entry concerned from the above-mentioned access permit list.

[0015] Moreover, the network connection control approach of this invention When accessing the service currently provided with the local network side from the device by the side of global network, The step which is the network connection control approach of performing control which permits or refuses the access concerned, and attests to the device by the side of the above-mentioned global network, When a data packet is received to access of a device by which authentication was carried out [above-

mentioned] from the step which generates an access-permission entry and adds the access-permission entry concerned to an access permit list, and the device by the side of the above-mentioned global network, Based on the information extracted from the header of the data packet concerned, and the access-permission entry contained in the above-mentioned access permit list, it has the step which judges whether the data packet concerned is transmitted to a local network side.

[0016] Moreover, in this invention, suitably, when generating the above-mentioned access-permission entry, access information is extracted from the access request packet transmitted from the device by which authentication was carried out [above-mentioned], and the access-permission entry containing a transmitting agency IP address, a destination IP address, a transmitting agency port number, a destination port number, and the last access-permission time of day is generated.

[0017] Furthermore, in this invention, when a transmitting agency IP address, a transmitting agency port number, a destination IP address, and a destination port number are suitably extracted from the header of the data packet transmitted from the device by the side of the above-mentioned global network, the extracted information concerned is compared with the information on the access-permission entry contained in the access permit list and all of a transmitting agency IP address, the IP address of the destination, a transmission place port number, and a destination port number are in agreement, the data packet concerned is transmitted to a local network side.

[0018]

[Embodiment of the Invention] 1st operation gestalt drawing 1 is the block diagram showing an example of the network system containing the network connection control unit concerning this invention. This network system is constituted like illustration by the gateway 30 connected between global network (WAN:Wide Area Network) 10, a local network (LAN:Local Area Network) 20, global network 10, and a local network, the terminal equipment 40 connected to global network 10, and the terminal equipment 50 connected to the local network 20.

[0019] The gateway 30 is the so-called network connection control unit which has the fire wall function to permit the access, only to the attested terminal equipment, when the access request to the service from the terminal equipment by the side of global network 10 currently offered by the local network 20 side is received. In addition, although one terminal equipment is connected to global network 10 and a local network 20 at a time in drawing 1 , respectively, many terminal equipments are usually connected to global network 10 and a local network 20 in the actual network system, respectively.

[0020] The fire wall is prepared in the gateway 30 and access to the terminal equipment by the side of a local network 20 by the side of global network 10 from a terminal equipment is not permitted in usual. Moreover, inside the local network 20, the respectively private IP address is assigned to each terminal equipment, and at least one global IP address is assigned to the global-network connection interface of the gateway 30. Each terminal equipment by the side of a local network 20 accesses the service which a global-network side offers using an IP masquerade technique.

[0021] By the access request from the device attested among the terminal equipments connected to global network 10 by the network system constituted in this way, this invention permits access to the service by the side of the local network 20 which specified only the device, refuses access from the device by the side of other global network, namely, offers the network connection control unit which can be changed dynamically for a fire wall setup.

[0022] In addition, in the following explanation, the message at the time of notifying to the gateway 30 giving [which the terminal equipment by the side of global network 10 wishes] is called "service access demand message" for convenience. Moreover, in the local network 20 side, since the private IP address is used, the port number is assigned to the gateway 30 for every service so that the service currently offered by the local network 20 side can be specified from the device by the side of global network. The device by the side of global network 10 can access giving [to wish one's service] by specifying the global IP address and port number of the interface by the side of the global network in the gateway 30.

[0023] Here, when the device by the side of a "service IP address", a "service port number", a call, and global network accesses an IP address and a port number for the device by the side of global network to specify the service by the side of a local network for convenience at the device by the side of a local

network, respectively, these service IP addresses and service port numbers are included in a service access demand message, and it transmits to the gateway 30.

[0024] Drawing 2 is the block diagram showing the configuration of the gateway 30. Hereafter, the configuration and function of each part of the gateway 30 are explained, referring to drawing 2. The gateway 30 is constituted by the access-control section 31, the address translation section 32, the global-network (WAN) side interface section 33, the local network (LAN) side interface section 34, and the storage section 35 like illustration. Furthermore, the access section 31 is constituted by the analysis section 301, the authentication section 302, and the list Management Department 303.

[0025] The access-control section 31 analyzes the service access demand message which received from the global-network side, attests a device, and manages an access permit list. Moreover, according to the result of the analysis and authentication, the authorization or refusal of access of a data packet received from the global-network side is controlled.

[0026] Hereafter, each component of the access-control section 31 is explained. The analysis section 301 analyzes by extracting required information from the data packet which received by the WAN side interface section 33. For example, if a service access demand message is transmitted from the device by the side of global network to the device by the side of a local network, this message will receive by the WAN side interface section 33, and will be passed to the access-control section 31. In the access-control section 31, from the service access demand message which received, information, such as a transmitting agency IP address, a port number and a destination IP address, and a port number, is extracted by the analysis section 301, an access-permission entry is generated based on it, and it is sent to the list Management Department 303.

[0027] Moreover, the analysis section 301 extracts information, such as an IP address of a transmitting agency and the destination, and a port number, from the header of a data packet received by the WAN side interface section 33, and opts for authorization or refusal of access based on the extracted information concerned and the information on the access-permission entry contained in an access permit list.

[0028] The authentication section 302 attests according to the authentication approach and authentication procedure which were beforehand set up to the device concerned, when a service access demand message is received from the device by the side of global network 10. And the information about the attested device is transmitted to the analysis section 301, and the access-permission entry to the access is created by the analysis section 301.

[0029] The list Management Department 303 adds the access-permission entry created by the analysis section 301 to reception and the access permit list memorized by the storage section 35. Or when access termination is carried out, the access-permission entry corresponding to the access is deleted from the access permit list memorized by the storage section 35.

[0030] The address translation section 32 is required only when the private IP address (or it is called a local IP address) is used for the local network 20 side. That is, the address translation section 32 changes the global IP address currently used by the global-network 10 side, and the local IP address currently used by the local network 20 side.

[0031] The WAN side interface 33 transmits and receives a packet to global network 10. That is, the packet transmitted from global network 10 is received, and the packet generated by the access-control section 31 by delivery and the access-control section 31 is transmitted to global network 10.

[0032] The LAN side interface 34 transmits and receives a packet to a local network 20. That is, the packet transmitted from the local network 20 is received, and the packet sent to the address translation section 32 from delivery and the address translation section 32 is transmitted to a local network 20.

[0033] The storage section 35 memorizes an access permit list. The access permit list concerned is managed by the list Management Department, the access-control section 31. The access-permission entry of access which the access-permission entry generated by the analysis section 301 was added to the access permit list concerned, and was ended is deleted from the access permit list concerned.

[0034] Hereafter, actuation of the access-control section 31 of the gateway 30 in this operation gestalt is explained. First, from the device by the side of global network 10, when the "service access demand

message" the "service IP address" and the "service port number" were indicated to be is received from the WAN side interface section 33, actuation of the access-control section 31 is explained.

[0035] Drawing 3 is a flow chart which shows actuation of the access-control section 31 when receiving a "service access demand message." As shown in drawing 3, the service access demand message which received from the WAN side interface section 33 is received first (step S1). And the starting point IP address and starting point port number which show the device and interface of the transmitting side indicated by received IP header of a service access demand message are checked, and it attests about the device which transmitted the service access demand message concerned (step S2). In addition, by this invention, although the approach of attesting a device can consider authentication by IPsecAH, the 3rd person authentication by Kerberos, etc., since it is realizable by the existing approach, authentication of this transmitting-side device is not limited especially here.

[0036] When authentication goes wrong, the "service access demand message" is discarded (step S3), and processing is ended. Conversely, when it succeeds in authentication, processing shown below is performed.

[0037] When authentication is successful, four information, the starting point address of IP header, IP header starting point port number, the service IP address number indicated by the payload, and the service port number indicated by the payload, is extracted from the "service access demand message", respectively.

[0038] And four information by which the extract was carried out [above-mentioned] is stored in four storage regions (field), an authorization starting point IP address field (ASIP), an authorization terminal point IP address field (ADIP), the authorization starting point port number field (ASPT), and the authorization terminal point port number field (ADPT), respectively, and an "access-permission entry" is created (step S4).

[0039] There is "the last access-permission time-of-day field (LATM)" which stores in an access-permission entry the time of day when using this entry and relaying a packet from a global-network 10 side to a local network 20 side at the end in addition to the four fields mentioned above, and when it is new creation, the time of day which created that access-permission entry is stored in the field concerned.

[0040] And the "access-permission entry" created as mentioned above is added to an "access permit list" (step S5).

[0041] An example of the access-permission entry generated by the processing mentioned above is shown in drawing 4. The address which the global IP address of a device which transmitted the service access demand message, 131.113.82.1 [for example,], is stored in an authorization starting point IP address field (ASIP) in the entry concerned like illustration, and shows the destination of a service access demand message to an authorization terminal point IP address field (ADIP), for example, the global IP address currently assigned to the interface section 33 by the side of WAN of the gateway 30, and 210.139.255.223 It is stored. (Moreover, the port number of a device which transmitted the service access demand message to the authorization starting point port number field (ASPT), for example, 20010, It is stored and 5000 is further stored in the authorization terminal point port number field (ADPT) here [the port number and here] where the destination of a service access demand message is shown.) Moreover, 21:10:10 which is the time of day which created the entry is stored in the last access-permission time-of-day field (LATM).

[0042] The access-permission entry shown in drawing 4 is added to an access permit list. In addition, the access permit list concerned is managed by the access-control section 31, for example, is memorized by the storage section 35.

[0043] Next, it explains, referring to the flow chart shown in drawing 5 about actuation of the access-control section 33 by the WAN side interface section 33, when a data packet is received from global network 10.

[0044] First, a data packet is received from the WAN side interface section 33 (step SS 1). Four information is extracted for the starting point IP address (SIP) of IP header, the terminal point IP address (DIP) of IP header, the starting point port number (SPT) of a TCP/UDP header, and the terminal point

port number (DPT) of a TCP/UDP header from the data packet which received, respectively.

[0045] And with reference to the access permit list currently held at the storage section 35, ASIP is equal to SIP, ADIP is equal to DIP, ASPT is equal to SPT, and it checks about whether an access-permission entry with ADPT still more nearly equal to DPT exists. According to the result of the check concerned, it opts for authorization or refusal of passage to the data packet which received (step SS 2).

[0046] In the above-mentioned check, when all the fields are not in agreement, passage of a data packet is not permitted but this data packet is discarded (step SS 3).

[0047] On the other hand, when the access-permission entry all whose fields correspond exists in the above-mentioned check, passage of the data packet which received is permitted. Current time of day is stored in the last access-permission time-of-day field (LATM) of the corresponding access-permission entry at this time (step SS 4). In addition, current time of day here is time amount shown by the time management section which is managed by OS (operation system) of the gateway 30, and is usually called a system clock.

[0048] After updating the last access-permission time-of-day field, the data packet which received is transmitted to the address translation section 32 (step SS 5). And in the address translation section 32, the global IP address in IP header of a data packet is changed into the local IP address currently used inside the local network 20, and is transmitted to the LAN side interface section 34. Concretely, DIP and DPT are changed into the local IP address and port number of a device which actually offer service by the local network 20 side, respectively. It is transmitted to a local network 20 by the LAN side interface section 34, and the changed data packet is transmitted to the device which actually offers service.

[0049] When it is going to access the service currently offered by the local network 20 from the device by the side of global network 10 by the processing mentioned above, the starting point, the terminal point IP address and the starting point contained in IP header of a data packet, and TCP / UDP header received by the gateway 30, and terminal point port number information are extracted, it is based on a comparison result with the access permit list memorized by the extracted information and the storage section 35 concerned, and it is determined whether to permit or refuse access. When the access concerned is refused, a data packet is discarded, and when the access concerned is permitted conversely, the destination of a data packet is changed into the local IP address of a device which is used by the local network 20 and which carries out service provision by the address translation section 32, and is transmitted to a local network 20 side through the LAN side interface section 34.

[0050] For this reason, since only access from the attested device is permitted and access from the other device is refused when accessing the service currently offered by the local network 20 side from the device by the side of global network 10, the security nature of a fire wall improves, injustice can refuse access, and also access from the attested device is permitted and high service of convenience can be offered to the user of normal.

[0051] The access permit list formed of the access-permission entry of access permitted to the storage section 35 by processing mentioned above is memorized. In the gateway 30, a judgment whether based on the access permit list concerned, IP header of the received data packet, and TCP/UDP header information, the received data packet is transmitted to a local network 20 side is made. Since a new access-permission entry is created to the access whenever access is established, and it is added to an access permit list, it increases according to the number of accesses which the capacity of an access permit list received. Furthermore, in order that the access-permission entry about access which received authentication once may remain in the access permit list of the storage section 35 eternally even when the access is completed even if it leaves an access-permission entry to an access permit list as it is, there is a security top problem. For this reason, it is necessary to delete that access-permission entry at any time to ended access.

[0052] Drawing 6 is a flow chart which shows the processing which deletes an access-permission entry based on the last access-permission time of day and threshold level time amount. Hereafter, the deletion of an access-permission entry is explained with reference to drawing 6.

[0053] This deletion is the elapsed time tD from the last access-permission time of day to current (at the time of decision) time of day. Threshold level time amount TS set up beforehand It compares and is

elapsed time tD as a result of a comparison. Threshold level time amount TS When it exceeds, that access-permission entry is deleted from an access permit list. That is, even if it goes through fixed time amount from the last access, when there is no new access, the authorization to the access is canceled. In addition, this deletion is performed to the all entry in an access permit list for every fixed time amount of a certain.

[0054] As shown in drawing 6 , it is the value t_f of an access-permission entry to the last access-permission time-of-day field (LATM) first. It is read (step SP 1). And the elapsed time $tD (= t - t_f)$ from the difference, i.e., last access-permission time of day, of the present time of day t and the time of day t_f read from the last access-permission time-of-day field to current is calculated. The elapsed time tD concerned Threshold level time amount TS It is compared (step SP 2).

[0055] Elapsed time tD Threshold level time amount TS When small, nothing is processed to the access-permission entry (step SP 3). Elapsed time tD Threshold level time amount TS Equally, when larger, the access-permission entry is deleted from an access permit list (step SP 4).

[0056] It is the elapsed time tD from the last access time by the processing mentioned above.

Predetermined threshold level time amount TS When it exceeds, the access-permission entry is deleted from an access permit list. That is, when it has gone through fixed time amount from the last access and there is no access, it is regarded as what ended the access, and an access-permission entry is deleted. In addition, threshold level time amount TS It can be set as a different value for every access-permission entry. For example, it is related with access to a WWW server, and is the threshold level time amount TS of an access-permission entry. Threshold level time amount TS of the access-permission entry set up short and concerning Telnet and FTP It can set up for a long time.

[0057] Drawing 7 is a flow chart which shows the processing which deletes the access-permission entry formed to the access from an access permit list, when the notice of access termination is received from the side to access. Hereafter, this deletion is explained, referring to drawing 7 .

[0058] Like illustration, a data packet is first received from the WAN side interface section 33 (step SQ1). Next, a judgment is made about whether the information (henceforth access termination information for convenience) which shows termination is included in the received data packet (step SQ2).

[0059] When access termination information is not included as a result of the decision concerned, the usual processing is performed to a data packet (step SQ3). On the other hand, when access termination information is included in the data packet as a result of the decision concerned, the access-permission entry according to the access concerned is deleted from an access permit list (step SQ4).

[0060] When access termination information is included in the data packet which received by the processing mentioned above, the access-permission entry formed when the access was established is deleted from an access permit list. For this reason, since the access-permission entry currently formed when access was completed according to this and that access was established is immediately deleted from an access permit list when termination of access is directed from the device by the side of global network 10, it can prevent that that entry is abused after access termination, and is desirable on security.

[0061] When a certain constant value is exceeded, it becomes impossible moreover, to store the number of the access-permission entries in an access permit list, since the resource of the gateway 30 is limited. For this reason, out of the access permit list currently held when an access-permission entry new in the situation of $\max [\text{number} / \text{of access-permission entries}]$ is added, an access-permission entry with the oldest value of the last access-permission time of day of an access-permission entry can be deleted, and a new access-permission entry can be added.

[0062] As mentioned above, although two kinds of entry deletion in the network connection control unit 30 of this operation gestalt, i.e., the gateway, was explained, entry deletion of the gateway 30 can also be performed by other processings, without being restricted to this. For example, terminating access is also considered based on decision of the processing which terminates access compulsorily based on decision of the gateway 30, or the device which actually provides the local network side with service.

[0063]

[Effect of the Invention] As explained above, according to the network connection control unit and its

control approach of this invention, in the gateway equipped with the fire wall function, it is permitted that only the device by the side of the permitted global network accesses the service by the side of a local network, and a network user can use easily the service currently offered by a certain local network from the network of a migration place if needed. On the other hand, access from other users' device can be refused by setup of the fire wall of the gateway, and there is an advantage which can maintain the security level by the side of a local network.

[Translation done.]